Dear Colleague,

We have been made aware of spam emails circulating into the Trust that contain links to external websites. These external websites contain the HSC logo and login boxes prompting for username and password or download a malicious file. We would ask that you remain extremely vigilant when receiving any emails that contain links or attachments even if it is from someone you regularly receive emails from. We have observed several users within this Trust attempt to visit these websites as a result of clicking on fraudulent links but fortunately our defences have prevented on this occasion. Given the continually evolving and persistent nature of these threats our defences cannot block 100% of spam emails. We would also like to take this opportunity to remind you of how you can help avoid being the victim of a cyber-attack both at home and work:

1. 'Think before you click'. Are you expecting the email? and who is it from?. Remember that you can hover over any links without clicking them to see where they point to.

2. Treat **ALL EMAILS** with caution.

3. Keep passwords strong, private and update them often.

4. Don't click on suspicious links or attachments. This can lead you to download malware, a virus or alert the attackers to the fact that you have clicked a link and that your email address is targetable.

5. Don't reply to suspicious emails. This lets the attackers know that your email address is targetable.

6. If you aren't sure – ask for help. If need be you can verify the legitimacy of an email sender in person.

7. Don't open unexpected attachments.

8. Stay alert and report suspicious activity to IT. You can forward any emails you suspect as spam to **spam@southerntrust.hscni.net**

9. Don't give away confidential or personal information – by phone, email, or social media.

10. If you receive an unexpected call whereby someone is claiming an IT issue with your computer system and asking you to navigate to a particular website and to download software – please end the call. The Trust IT team will never ask you to download software from external websites or to go to a website and ask you to login. Also, the Trust IT team will never ask you for your username and password through email communications.

11. Don't leave your device unattended while logged in. Lock, log off and shutdown.

12. Be careful what you plug into your computer (smart phones and flash drives can contain malware).

13. Install anti-virus software and keep all computer software updated with the latest patches *(at home – the Trust IT team will look after your work related devices in this respect).*

14. Don’t use free public WIFI when logging in to your bank or other important services. Fraudsters can intercept your data.

15. Backup your important home information.